

不正アクセス手法と技術的対策に関する調査

不正アクセス環境別詳細対策集

平成 13 年 3 月

情報処理振興事業協会

目次

1. <u>WINDOWS 環境における不正アクセス対策</u>	1
1.1. <u>対策の概要</u>	1
1.1.1. <u>Windows 環境における不正アクセス対策の概要</u>	1
1.1.2. <u>対策情報の入手</u>	2
1.1.3. <u>修正プログラムの適用方法</u>	5
1.2. <u>WINDOWS オペレーティングシステムの脆弱性とその対策</u>	6
1.2.1. <u>パスワードの不正入手への対策</u>	6
1.2.2. <u>管理者権限の不正取得への対策</u>	7
1.2.3. <u>サービス妨害攻撃への対策</u>	10
1.2.4. <u>受動的攻撃への対策</u>	14
1.3. <u>WINDOWS 環境のセキュリティ管理</u>	16
1.3.1. <u>Windows NT 4.0 Server / IIS4.0 のセキュリティ対策設定</u>	16
1.3.2. <u>より厳しいセキュリティ対策設定</u>	18
1.3.3. <u>Windows 2000 Server / IIS 5.0 のセキュリティ対策設定</u>	20
2. <u>LINUX 環境における不正アクセス対策</u>	21
2.1. <u>対策の概要</u>	21
2.1.1. <u>Linux 環境における不正アクセス対策の概要</u>	21
2.1.2. <u>対策情報の入手</u>	21
2.1.3. <u>その他のベンダが提供する UNIX のセキュリティに関する情報</u>	24
2.2. <u>RED HAT LINUX オペレーティングシステムの脆弱性とその対策</u>	25
2.2.1. <u>管理者権限の不正取得への対策</u>	25
2.2.2. <u>サービス妨害攻撃への対策</u>	26
2.3. <u>RED HAT LINUX のセキュリティ管理</u>	27
2.3.1. <u>デフォルトのアカウントに関する修正</u>	27
2.3.2. <u>既知のセキュリティホールの修正</u>	27
2.3.3. <u>不要なサービスの停止と削除</u>	27
2.3.4. <u>root のセキュリティ</u>	28
2.3.5. <u>TCP wrapper によるサービスへのアクセス制限</u>	29
2.3.6. <u>ssh の利用</u>	29
2.3.7. <u>メール関連設定</u>	30
2.3.8. <u>Web 関連設定</u>	32

1. Windows 環境における不正アクセス対策

Windows 環境における不正アクセス対策について以下に述べる。

1.1. 対策の概要

1.1.1. Windows 環境における不正アクセス対策の概要

Windows 環境で十分なセキュリティを確保するためには、Windows NT4.0 / Windows 2000 を

プラットフォームとして選択する必要がある。Windows 9x オペレーティングシステムは OS レベルでのセキュリティ制御が弱く、将来のセキュリティ制御面の強化も期待できない。

Windows NT4.0/2000 オペレーティングシステムは適切に利用すれば非常に高い安全性を実現できる。しかしながら、セキュリティを確保するためには、詳細な設定を行い、厳密な利用基準に従う必要がある。Windows NT 4.0/2000 のセキュリティ強化措置の前提条件としては、少なくともハードディスクを NTFS 形式でフォーマットし、アクセス制御リストをファイルシステムに適用する必要がある。また、最新のサービスパック (SP) と SP がサポートしていない全ての修正プログラムを適用しなければならない。

経験の浅い管理者による Windows 環境のセキュリティ管理には多くの困難が伴う。以下にその理由をいくつか挙げる：

- ・ ネットワーク関連仕様の曖昧さと複雑さ。Windows 製品においては頻繁にセキュリティモデルの変更が行われる。新規のモデルにおいても下位互換性を保つために随所でセキュリティ面の譲歩が行われるため、よりいっそう複雑性が増す。下位互換性に由来する問題と思われる例を挙げる：
 - Windows NT 環境における NetBIOS、CIFS、SMB ネットワークへの継続的な依存
 - 明白な脆弱性が指摘されている LanManager アルゴリズムによるユーザパスワードの暗号化の一貫したサポート
- ・ Windows 環境では単一のサーバによる複数の高度なサービスの提供が意図されている。各サービスが相互に複雑に関係し合う実装が施されているため、サーバの役割に応じた必要最小限の機能構成を設定する方法が判り難く、必要な機能と不要な機能の分離が困難である。動作するサービスを管理者が見落とすことも多く、セキュリティホールの放置に繋がりがやすい。また、この複雑さがセキュリティホールの発生を未然に防ぎ難くしている。
- ・ セキュリティに関するデフォルト設定が緩く作られている。このため「許可したもの以外は全て禁止する」方針の徹底が非常に難しく、管理者の知識不足により見落とされ得るセキュリティホールが多数存在する。

1.1.2. 対策情報の入手

システムのセキュリティ担当者は、セキュリティ対策関連情報を複数の情報源から習慣的に収集し、自らの管理するシステムに合わせて適用する必要がある。管理対象のシステムで利用している OS やサービスプログラムに関しては以下のような情報を収集する。

- ・ 適切なセキュリティ設定を示すドキュメント
- ・ 脆弱性情報
- ・ 修正プログラム
- ・ 最新の攻撃手法の動向

修正プログラムについては、適用する正しい順序、適用によって起き得るトラブルとその対策、修正対象に関する技術的情報なども集める。修正プログラムに不具合が発見されることも珍しくはないので、修正後も確認が必要である。

サーバ製品は導入時に製品ベンダのサイトを参照し、脆弱性に関する情報の場所と更新頻度を確認しておくべきである。ユーザ登録により連絡を受けられるように取り計らうことや、サポート情報のチェックを習慣的に行うことが必要である。

特に悪用の危険性の高い脆弱性については、情報が公開されてから修正プログラムが公開され、これを適用して安全性が確保されるまでの間は、情報収集と吟味を継続的に行うべきだろう。

これまでに良く知られた脆弱性への対策や、サーバ導入時に必要な対策に関する情報源としては以下のサイトが利用できる。

マイクロソフトサイト

(1) TechNet Online – Security

URL : <http://www.microsoft.com/japan/technet/security/default.asp>

セキュリティ関連情報のサイト。修正プログラム情報以外にも、セキュリティに関する最新の動向情報、Windows システムの適切な設定方法のガイド等、有用な記事へのリンクが多数掲示されている。更新のペースは非常に早いので、システム管理者は頻繁に（少なくとも日に 1 回程度は）確認すると良いだろう。

(2) TechNet Online - マイクロソフト セキュリティ情報

URL : <http://www.microsoft.com/japan/technet/security/current.asp>

上述したマイクロソフトのサイトに含まれる、マイクロソフトが確認した脆弱性に対する修正プログラムと関連情報の一覧を示すページ。

修正プログラムには通し番号「MSyy-nnn」が与えられている（yy は西暦下二桁、nnn はそ

の年に登録された順に振られるナンバー)。この番号は全ての製品を通して一意に振られる。関連する複数の脆弱性を1つのプログラムで修正する場合は、相互に関連して問題を起こすかどうかには関わらず、まとめてひとつの番号で数えている。2000年にマイクロソフト社からは100件の脆弱性とその対応策が報告されている

個々の脆弱性対策を説明するフォーマットは以下のように構成されている。

- ・ 概要
修正プログラムのリリース状態と、攻撃が成功する結果によって受け得る影響が簡潔に示されている。
- ・ 詳細な情報(よく寄せられる質問)へのリンク
「よく寄せられる質問(FAQ)」情報がある場合はリンクが張られている。FAQでは脆弱性の影響する範囲までを含めた技術的詳細が丁寧に解説されている
- ・ 問題
問題点の明確化、より詳細な影響についての説明が行われる。
- ・ 修正モジュールへのリンク
この項目でプロダクト、OSのバージョンごとに日本語版修正プログラム・ツールへのリンク、あるいは準備状況が示されている。
- ・ 該当するプロダクト
脆弱性が存在するプロダクトの名前が示されている。
- ・ 詳細情報へのリンク
上記の「よく寄せられる質問」へのリンク以外に、USマイクロソフトの当該ページへのリンク、サポート技術情報(ナレッジベース:KB)文書へのリンクが示されている。

(3) Microsoft TechNet Security (英語)

URL : <http://www.microsoft.com/technet/security/default.asp>

米 Microsoft のサイト。英語版の Windows NT / 2000 をインストールしている場合はここからリンクを辿って英語版の修正プログラムを入手する必要がある。

Windows セキュリティ情報に関するサイト

(1) NT Security

URL : <http://www.port139.co.jp/ntsec.htm>

NT の脆弱性に関する総合的な情報サイト。IIS4.0/5.0 インストール時のセキュリティ対策サマリ、不正アクセス手法と対策ツールの紹介、チェックリスト等が公開されている。

(2) Win セキュリティ虎の穴

URL : <http://winsec.toranoana.ne.jp/>

マイクロソフトより提供される対策情報へのリスト（更新順）が含まれる。日本語版修正プログラムの有無、適用方法に関する簡潔なメモが付けられている。セキュリティ関連ニュースへのリンクが含まれる。

1.1.3. 修正プログラムの適用方法

原則として、セキュリティ修正プログラムは古いものから順に適用する。管理対象マシンごとに適用した修正プログラム名・修正を施した日付についての記録を取り、後に参照できるようにしておく必要がある。サービスを追加した際や、システムの部分的な再インストールを行った際は、遡って古いパッチを適用する必要があるが生じる。

OS の更新（サービスパックの適用）については、既存の修正プログラムのうちでこれに含まれるものを確認し、不足している修正プログラムは古いものから順にこれを適用する。

Windows 環境においてはデフォルトのシステム設定やベンダが推奨されるシステム設定は、セキュリティが緩く設定される傾向にある。このため、設定の修正・確認を行わずに安易な運用を行うと本来は機能上達成可能なセキュリティを満たすことができない。設定の変更や新たな機能を導入する際には、識者コメント等の複数の情報源を参考に吟味を加えた上で、システムに対して最小限の変更を行う必要がある。

1.2. Windows オペレーティングシステムの脆弱性とその対策

1.2.1. パスワードの不正入手への対策

パスワードは初歩的なセキュリティ手法と受け取られることもあるが、現実的には、ほぼ唯一のユーザ認証手段であり、その管理を徹底する必要がある。

パスワードの奪取に繋がる不正アクセス手法については、その脆弱性の特徴によっていくつか分類可能である。以下にそれらを記す。

- ・ 弱い権限でも取得可能な位置に置かれたファイルにパスワードが書かれている場合
- ・ 脆弱なアルゴリズムや誤った実装によるパスワードの暗号化処理が施されている場合
- ・ パスワードが平文でファイルに書かれている場合や、平文で送受される場合

たとえ暗号化されたファイルにパスワードが保存されていても、攻撃者がこれを入手すれば辞書攻撃あるいは総当たり攻撃（ブルートフォース攻撃）により解読が可能である。辞書攻撃を避けるためには、類推が容易なパスワードを避ける等のユーザによる工夫が求められる。

個々のマシン管理者のパスワードやサービス管理者のパスワードをシステム管理者のパスワードと同一にしてしまうと、1つのパスワードの露呈によってシステム全体に危険が及ぶ。

以下に Windows NT / Windows 2000 におけるパスワードに関連する脆弱性を挙げる。

(ア) デスクトップの分割による脆弱性 (CVE-2000-0475)

- ・ 対象：Windows 2000
- ・ 手法：ある特定の環境においてユーザが別のデスクトップでプロセスを生成できる。
- ・ 影響：攻撃者は同一セッション内のデスクトップで実行されている入出力処理を、低い権限を持つユーザのプロセスから参照し、パスワード情報などを取得可能。
- ・ 予防対策：修正プログラムの適用。

(イ) telnet クライアントにおける NTLM 認証に関する脆弱性 (CVE-2000-0834)

- ・ 対象：Windows 2000
- ・ 手法：出荷時の設定では telnet.exe クライアントが、ホストとの接続時に相手が Windows telnet サーバであるかどうかに関わらず Windows NT Challenge/Response 手法での認証を試みる。この認証に用いられる LanMan ハッシュアルゴリズムはブルートフォース攻撃に対して非常に脆弱であることが広く知られている。
- ・ 影響：リモートからの攻撃者は、悪意ある Web サーバを用いるなどして、ユーザ名、パスワード、ドメイン名等の機密性を有する情報を不正に取得可能。
- ・ 予防対策：修正プログラムの適用。2000年9月16日に更新された最新パッチの適用が必要。NTLM 認証を無効化することも有効。

1.2.2. 管理者権限の不正取得への対策

ここでは Windows オペレーティングシステム自体に存在する脆弱性について取り上げる。Windows に存在する脆弱性のうち、管理者権限の不正取得に繋がるものの多くは、ローカルな攻撃者のみが利用可能な脆弱性である。この傾向が見られる理由としては、ユーザによるプログラムの実行が基本的にクライアント上で行われ、Windows NT サーバ上でプロセスが実行されることが少ないという、Windows ネットワークにおけるプロセス実行の特異性が挙げられる。

以下に Windows NT / Windows 2000 オペレーティングシステムにおいて、管理者権限の不正取得に繋がる脆弱性の例を、リモートからの攻撃手法、ローカルな攻撃手法に分けて述べる。

リモート攻撃

(ア) Windows 2000 インストール時の保護されていない ADMIN\$ Share に関する脆弱性 (CVE-2000-0222)

- ・ 対象：Windows 2000
- ・ 手法：システムが再起動されるまで管理者のパスワードをインストーラが有効にしない。
- ・ 影響：リモートからの攻撃者は再起動が起こるまでの間、ADMIN\$シェアにパスワード無しで接続可能。
- ・ 予防対策：2001年3月現在、特に対応策は無い。

(イ) Windows NT 4.0 ターミナルサーバーのログオンにおけるバッファオーバーフロー脆弱性 (CVE-2000-1149)

- ・ 対象：Windows NT 4.0
- ・ 手法：ログオンプロンプト (RegAPI.DLL) に適切なチェックが行なわれないバッファがあり、ログイン時に長いユーザ名を入力するとバッファオーバーフローを起こせる。
- ・ 影響：リモートからの攻撃者はサービス妨害、管理者権限での任意の命令実行が可能。
- ・ 予防対策：ベンダの提供する修正プログラムの適用。インターネットからターミナルサーバーにアクセスする必要がない場合はファイアウォールあるいはルータを設定してポート 3389 をブロックする。

ローカル攻撃

(ウ) 偽装 LPC ポートリクエストに関する脆弱性 (CVE-2000-0070)

- ・ 対象：Windows NT 4.0
- ・ 手法：LPC ポートにおける、同一マシン上でサーバスレッドがクライアントスレッドを模倣する API 機能に脆弱性が存在する。クライアントとサーバスレッドの両方を作成し、システムを含むローカルマシン上で偽装リクエストを任意のユーザコンテキストで操作できる。
- ・ 影響：ローカルな攻撃者はローカルマシン上の管理者権限の取得、監査ログの記載の改竄、他のユーザへのなりすまし、任意のコードの実行が可能。
- ・ 予防対策：修正プログラムの適用

(エ) Shell の相対パスの脆弱性 (CVE-2000-0663)

- ・ 対象：Windows NT 4.0、Windows 2000
- ・ 手法：実行可能ファイルや DLL がその位置をレジストリ内でパス指定されない場合は、アプリケーションがロードされたディレクトリ、親プロセスが現在実行されているディレクトリ、..¥System32、..¥¥System、Windows ディレクトリ、PATH 環境変数で指定されたディレクトリ、の順に検索がかけられ、該当するファイル名のファイルがあればオープンされてしまう。
- ・ 影響：ローカルな攻撃者は、トロイの木馬プログラムを仕掛け、他のユーザがログオンした際に任意のコードを実行させることが可能。
- ・ 予防対策：修正プログラムの適用

(オ) サービスコントロールマネージャの名前付きパイプを利用したなりすましに関する脆弱性 (CVE-2000-0737)

- ・ 対象：Windows 2000
- ・ 手法：システムサービスのために名前付きパイプを作成するサービスコントロールマネージャ (SCM)機能に問題があり、特定のサービスの、次のインスタンスの名前を予測できる。サーバ側にそのサービスのための名前付きパイプを事前に作成し、その特定のサービスが次に実行されたときに、パイプに付加したコードを実行することが可能。
- ・ 影響：ローカルな攻撃者は、あるサービスが次回開始された際に任意のコードを実行させることが可能。
- ・ 予防対策：修正プログラムの適用

(カ) 静止画像サービスを用いたアクセス権の向上に関する脆弱性 (CVE-2000-0851)

- ・ 対象 : Windows 2000
- ・ 手法 : 静止画像サービスに適切な入力のチェックを行っていないバッファがあり、長い WM_USER メッセージを用いてバッファオーバーフローを起こすことができる。
- ・ 影響 : ローカルな攻撃者は静止画像サービスの持つ権限 (デフォルトでは LocalSystem 権限) で命令を実行可能。
- ・ 予防対策 : ベンダの提供する修正プログラムの適用。

(キ) 簡体字中国語版 IME の脆弱性 (CVE-2000-0933)

- ・ 対象 : Windows 2000
- ・ 手法 : ログオン画面処理の間、簡体字中国語用の IME はユーザコンテキスト上ではなく LocalSystem コンテキスト (OS の権限) 上で動作し、ログオン以前にユーザが利用するのに適切でない機能が利用できる。よってユーザ名やパスワードを入力せずに LocalSystem コンテキストでログオンすることが可能となる。
- ・ 影響 : Terminal Server セッションやキーボードからアクセスできる攻撃者は、一切の証明を行わずにシステムに対する完全なアクセス権限を入手することが可能。
- ・ 予防対策 : ベンダの提供する修正プログラムの適用。

1.2.3. サービス妨害攻撃への対策

Windows システムに対するサービス妨害攻撃には以下のような意図があると考えられる。

- ・ サービスの妨害

サービス提供の効率の低下、あるいは中断を目的とした攻撃が行われる。

- ・ システムが停止後に再起動されることを意図した攻撃

一般に Windows システムに重要な変更を加えた際にはシステムのリブートが必要となる。侵入に成功した攻撃者が、特権を獲得するための仕事を完成させる際にもシステムの再起動が必要となることが多い。このような場合に、攻撃者が故意にサービス妨害攻撃を行い、正当な管理者によるシステムの再起動を促すことが考えられる。

以下に、WindowsNT/2000 オペレーティングシステムに存在する脆弱性に由来するサービス妨害攻撃の手法を示す。

ローカル攻撃

(ア) 不正な TCP/IP 印刷リクエストに関する脆弱性 (CVE-2000-0232)

- ・ 対象：Windows NT 4.0、Windows 2000
- ・ 手法：ネットワーク印刷サーバが不正な改ざんを受けた印刷リクエストを受信した場合、TCPSVC.EXE や DHCP 等のいくつかのサービスがクラッシュする。
- ・ 影響：ローカルなユーザはネットワーク印刷サーバに対するサービス妨害攻撃が可能。
- ・ 予防対策：修正プログラムの適用。

(イ) Active Directory オブジェクト属性に関する脆弱性 (CVE-2000-0311)

- ・ 対象：Windows 2000
- ・ 手法：あるディレクトリオブジェクトについてユーザがアクセス権を持つ属性を特殊な方法で変更する際に、オブジェクトの権限の無い属性を合わせて変更することが可能。
- ・ 影響：悪意あるユーザは権限の無い Active Directory 情報を改竄できる。
- ・ 予防対策：ベンダの修正プログラムの適用

リモート攻撃

(ア) 断片化した IP パケットの組み立て直しに関する脆弱性 (CVE-2000-0305)

- ・ 対象：Windows NT4.0、Windows 2000
- ・ 手法：断片化された IP データグラムが特定の方法で改ざんされ連続的に送信された場合、CPU 処理力の殆ど全てが消費され、マシンが一時的に応答を停止する。サーバのクラッシュが引き起こされる危険性もある。
- ・ 影響：リモートからの攻撃者はサービス妨害攻撃が可能
- ・ 予防対策：ベンダの修正プログラムの適用

(イ) cmd.exe のバッファオーバーフロー脆弱性 (CVE-2000-0331)

- ・ 対象：Windows NT 4.0、Windows 2000
- ・ 手法：コマンドプロンプト(CMD.EXE)の環境文字列を処理するコードに存在する問題。サーバにバッチファイルやスクリプトファイルなどが置かれている場合、極端に長い環境文字列を生成する引数を指定してバッファオーバーランさせることが可能。プロセスに割り当てられたメモリが使用できなくなり、サーバの応答の遅延や停止が起きる。特に Web サーバはリモートユーザのためにバッチファイルを置くためにこの脆弱性に基づく攻撃の影響を受け易い。
- ・ 影響：リモートからの攻撃者はサービス妨害攻撃が可能。
- ・ 予防対策：ベンダの修正プログラムの適用

(ウ) リモートレジストリアクセス認証に関する脆弱性 (CVE-2000-0377)

- ・ 対象：Windows NT 4.0
- ・ 手法：リモートマシンから他のマシンのレジストリへのアクセスリクエストに関する問題。改竄されたリクエストに対してリモートレジストリサーバが解釈を誤りプロセスがダウンする。これが元となってシステム全体がダウンする。
- ・ 影響：認証を受けた攻撃者はサービス妨害攻撃が可能。
- ・ 予防対策：ベンダが提供する修正パッチの適用

(エ) HostAnnouncement flooding 脆弱性 (CVE-2000-0403)

- ・ 対象：Windows NT 4.0
- ・ 手法：CIFS コンピュータブラウザプロトコルに関する問題。ブラウザリストのサイズを制御する機能が無いため、マスタブラウザに非常に多くの偽の HostAnnouncement フレームを送信された場合に、強制終了等に陥る。
- ・ 影響：攻撃者はブラウザサービスに対してサービス妨害攻撃が可能。
- ・ 予防対策：ベンダの提供する修正プログラムの適用。管理者は通常の管理ツールを使

用して攻撃者を特定可能。

(オ) AntiSniff DNS オーバフロー脆弱性 (CVE-2000-0405)

- ・ 対象：Windows NT4.0、Windows 2000
- ・ 手法：ある特定のテストにおいて DNS 仕様に忠実でないパケットが AntiSniff マシンに送られた場合にバッファオーバーフローが引き起こされる。
- ・ 影響：リモートからの攻撃者はサービス妨害を仕掛ける他、任意のコードを実行可能。
- ・ 予防対策：DNS テストを実行しないこと。商用バージョン 1.02 以降あるいは研究者用バージョン 1-1 以降へのアップデートを行うこと。

(カ) NetBIOS Name Server Protocol Spoofing の脆弱性 (CVE-2000-0673)

- ・ 対象：Windows NT4.0、Windows 2000
- ・ 手法：NetBIOS Name Server (NBNS) プロトコルの仕様では、WINS サーバだけでなく NetBIOS クライアントも名前重複の確認プロトコルにおいて認証が行われない。このため、WINS サーバを装って重複および名前解放のメカニズムを悪用できる。他のコンピュータの名前を重複しているものとして無効化し、応答を停止することが可能。
- ・ 影響：リモートからの攻撃者はサービス妨害攻撃が可能。
- ・ 予防対策：修正プログラムの適用

(キ) ローカルセキュリティポリシーの破壊に関する脆弱性 (CVE-2000-0771)

- ・ 対象：Windows 2000
- ・ 手法：改竄した RPC トラフィックを用いてローカルセキュリティポリシー (LSP) の機能を停止できる。クライアントにおいて LSP が破壊された場合は、ドメインにログオンできず、サーバからファイルを読み出せなくなる。ドメインコントローラにおいて LSP が破壊された場合は、ドメイン全体のネットワークサービスが完全に機能停止する。
- ・ 影響：リモートからの攻撃者はサービス妨害攻撃が可能。
- ・ 予防対策：修正プログラムの適用

(ク) Microsoft NetMeeting リモートデスクトップ共有におけるサービス妨害に対する脆弱性 (CVE-2000-0983)

- ・ 対象：Windows NT 4.0、Windows 2000
- ・ 手法：リモートデスクトップ共有を有効にしている場合に、NetMeeting ポート (1720 番) に null バイト入力列を送ると CPU 処理時間を浪費し、サービスは異常終了する。
- ・ 影響：リモートの攻撃者はサービス妨害攻撃が可能。通常の機能の回復に再起動が必

要。

- ・ 予防対策：ベンダの修正プログラムの適用。

1.2.4. 受動的攻撃への対策

各種サービスに関して外部からの攻撃への適切な対策を施されたシステムであっても、クライアントサイド（ユーザアプリケーション）のセキュリティに関して、適切な対策が採られていないことは多い。

Web に関するパケットは、多くの場合はファイアウォールやルータを素通しされ、何ら制限を受けずにブラウザ、メーラーといったユーザアプリケーションまで到達する（一部のファイアウォールの拡張機能にはスクリプトを無効化するフィルタ機能などもある）。これを利用して、ユーザアプリケーションに固有な脆弱性を狙い、クライアントマシン上での不正なプロセスの実行や情報の取得を試みる攻撃手法がある。これらの攻撃手法は、ブラウザやメーラーの脆弱性を利用し、サイト上に置かれたファイルやメールに添付された実行ファイルを、ユーザに無自覚のうちに実行させる攻撃（受動的攻撃）として知られている。

Windows 環境ではクライアントサイドのセキュリティについては特に注意を払う必要がある。Windows オペレーティングシステムと Microsoft 製ユーザアプリケーション群の間には密接な関係が築かれているため、受動的攻撃を受けやすい。

ブラウザやメーラーにおけるスクリプトや ActiveX コンポーネント等の拡張機能については、全くユーザに警告を与えずにプログラムが実行されるような脆弱性がいくつか報告されている。このような脆弱性を悪用した攻撃手法により、情報の漏洩、不正なコードのシステム権限による実行やインストール等が可能となる。

適切なセキュリティ対策を施さないままでユーザアプリケーションを管理者アクセス権で使用することは大変危険である。悪意あるサイト管理者が仕掛けた不正なコンテンツから管理者権限での受動的アクセスを避けるためには、管理者アカウントからの外部のサイトへのアクセスや電子メールの確認は行わず、必要時には管理者ではなくユーザとしてブラウズやメール処理を行うべきである。危険なスクリプトを含む文書や実行ファイルをダウンロードし、管理者アクセス権で実行した場合、管理者アカウントが奪われる可能性がある。

(1) Windows システムに対する受動的攻撃手法

以下に Windows オペレーティングシステムに対する受動的攻撃の手法の例を挙げる。

(ア) DOS デバイス名を含むパス名に関する脆弱性 (CVE-2000-0168)

- ・ 手法 : パスに DOS デバイス名が複数回含まれる場合、Windows95/98 はパスが不正であるというメッセージを返さずにファイルリソースとして解釈してしまう。この結果アクセス違反が発生し、システムがクラッシュする可能性がある。
- ・ 影響 : 攻撃者は、不正なパスを指定するハイパーリンクを張るなどして DOS デバイス名を含むファイルもしくはフォルダにアクセスするよう他のユーザを仕向け、サービス妨害攻撃が可能である。
- ・ 予防対策 : 修正プログラムの適用

1.3. Windows 環境のセキュリティ管理

Windows 環境のサーバ設定についてはベンダから適切な設定方法に関する細かな情報が提供されている。以下にその概要を示す。

1.3.1. Windows NT 4.0 Server / IIS4.0 のセキュリティ対策設定

Microsoft 社が推奨する Windows 4.0 Server の安全な設定方法を以下に示す。

参考：<http://www.microsoft.com/japan/technet/security/checklist.asp>

<http://www.microsoft.com/japan/technet/security/CheckListFurtherDetails.asp>

(1) Windows NT 4.0 の設定

以下の Windows NT オペレーティングシステムに関する設定を変更する。

- ・ 最新のサービスパックと修正プログラムを適用する
- ・ ハードディスクを最初から NTFS 形式でフォーマットする
- ・ NTFS Access Control List (ACL) に適切な設定を施す
- ・ NTFS での 8.3 形式の名前生成をオフにする レジストリの変更
- ・ システムの起動時間を 0 秒に設定する
- ・ スタンドアロンサーバとして設定する
- ・ OS/2 サブシステムを削除する
- ・ POSIX サブシステムを削除する
- ・ すべての Net Share を削除する
- ・ 成功/失敗したログオン/ログオフを監査する
- ・ 監査ログの上書き間隔を設定する
- ・ 最後にログオンしたユーザ名を非表示にする
- ・ ログオンの前に法的通知を表示する
- ・ [ログオン]ダイアログボックスから[シャットダウン]ボタンを削除する
- ・ パスワード長を設定する
- ・ Guest アカウントを無効にする
- ・ Administrator アカウント名を変更する
- ・ ユーザアカウント、グループメンバーシップ、および権限を確認する
- ・ Admin アカウントに推測困難なパスワードを設定する
- ・ 管理者のみがプリンタとドライブ文字を設定できるようにする
- ・ レジストリへの未認証アクセスを防止する
- ・ 匿名のネットワークアクセスを制限する
- ・ SYSKEY ユーティリティを実行する
- ・ [ネットワーク経由でコンピュータへアクセス]を[Everyone]から Authenticated

Users]に変更する

- ・ TCP/IP から NetBIOS をアンバインドする
- ・ IP ルーティングを無効にする
- ・ TCP/IP フィルタリングを構成する

(2) IIS 4.0 の設定

以下の IIS に関わる設定を変更する。

- ・ 必要最低限のインターネットサービスをインストールする
- ・ 適切な認証メソッドを設定する
- ・ 適切な仮想ディレクトリ権限/Web アプリケーション領域を設定する
- ・ 実行可能コンテンツの信頼性を確認する
- ・ IP アドレス/DNS アドレスの制約事項を設定する
- ・ 新しいルート証明を IIS に移行する
- ・ SSL (Secure Sockets Layer) を設定する
- ・ ログの記録を有効にする
- ・ Index Server がドキュメンテーションのみにインデックスを作成するようにする
- ・ Microsoft Certificate Server の Web サーバ登録用 ASP ページをロックする
- ・ IISADMPWD 仮想ディレクトリを削除する
- ・ RDS サポートを無効にする
- ・ すべてのサンプルアプリケーションを無効にする、または削除する
- ・ <FORM>入力をチェックする
- ・ 適切な仮想 IIS ログファイル ACL を設定する
- ・ SSI の#exec によるコマンドシェル呼び出しを無効にする
- ・ 親パス (「..」によるパス指定) を無効にする
- ・ 使われていないスクリプトマッピングを削除する

(3) ウイルス検索ソフトウェアのインストール

さらにサードパーティ製のウイルス対策ソフトウェアを導入することが望ましいとされる。

1.3.2. より厳しいセキュリティ対策設定

より厳しいセキュリティを実現するためのチェックリストとして、WindowsNT4.0 を C2 構成するためのチェックリストが示されている。

参考： <http://www.microsoft.com/japan/technet/security/C2config.asp>

セキュリティ強化対策として C2 構成のチェックリストには以下のような対策が示されている：

- ・ 電源をオンにするパスワードを設定する
- ・ ハードウェアの起動保護を有効にする
- ・ 「C2 Update」 hotfix をインストールする
- ・ NetBIOS インターフェイスサービスを削除する
- ・ 不要なデバイスを無効にする
- ・ 不要なサービスを無効にする
- ・ OS/2 および POSIX サブシステムを削除する
- ・ DirectDraw を無効にする
- ・ Guest アカウントを無効にする
- ・ ベースオブジェクトを保護する
- ・ NetBT を有効にして TCP ポートと UDP ポートを排他的に開く
- ・ その他の名前付きベースオブジェクトを保護する
- ・ カーネルオブジェクトの属性を保護する
- ・ ファイルとディレクトリを保護する
- ・ レジストリを保護する
- ・ 公開された LSA(Local Security Authority)情報へのアクセスを制限する
- ・ 名前付きパイプでのヌルセッションアクセスを制限する
- ・ 信頼されていないユーザが「トロイの木馬」プログラムを仕掛ける可能性を制限する
- ・ Administrator だけが新規共有を作成できるようにする
- ・ キャッシュへのログオン情報の一時保存を無効にする
- ・ プリンタドライバのインストールを Administrators と Power Users に限定する
- ・ ページファイルがシステムのシャットダウン時に除去されるように設定する
- ・ フロッピードライブと CD-ROM ドライブへのアクセスをインタラクティブユーザに限定する
- ・ ユーザ権利のメンバを変更する
- ・ ベースオブジェクト、およびバックアップと復元に監査を設定する（監査が有効の場合）
- ・ 空白のパスワードを無効にする

- ・ ログオンダイアログから[シャットダウン]ボタンを削除する
- ・ セキュリティログの動作を設定する

1.3.3. Windows 2000 Server / IIS 5.0 のセキュリティ対策設定

Windows 2000 Server / IIS 5.0 のためのセキュリティチェックリストが Microsoft から提供されている。

参考：

<http://www.microsoft.com/japan/technet/security/iis5chk.asp>

このチェックリストは Windows NT 4.0/IIS 4.0 のチェックリストに比べるとかなり短縮されている。これは以下のセキュリティ面での改良に基づく：

- ・ Windows 2000 のシステム全体に及ぶ設定の多くは、付属のセキュリティテンプレート (hisecweb.inf) により構成できるため、手動でレジストリ設定を構成する必要がない。
- ・ Windows NT 4.0 /IIS 4.0 における安全性が低いデフォルト設定のいくつかは、Windows 2000/IIS 5.0 ではデフォルトで無効に設定される。

以下の項目に関して修正を行う：

- ・ 付属の Hisecweb.inf セキュリティ テンプレートを確認、更新、および配備する
- ・ IPSec ポリシーを構成する
- ・ Telnet サーバを保護する
- ・ 仮想ディレクトリに適切な Access Control List (ACL) を設定する
- ・ 適切な IIS ログファイル ACL を設定する
- ・ ログの記録を有効にする
- ・ IP アドレスとドメイン名の制限を設定する
- ・ 実行可能なコンテンツは信頼性を検証して配置する
- ・ IIS サーバでルート CA 証明書を更新する
- ・ すべてのサンプルアプリケーションを無効または削除する
- ・ 不要な COM コンポーネントを無効または削除する
- ・ IISADMPWD 仮想ディレクトリを削除する
- ・ 未使用のスクリプトマッピングを削除する
- ・ ASP コードの FORM とクエリ文字列入力を確認する
- ・ 親パス (「..」を用いたパスの指定) を無効にする
- ・ コンテンツロケーションの IP アドレスを無効にする

2. Linux 環境における不正アクセス対策

Linux 環境における不正アクセス対策について、主に Red Hat Linux 環境のセキュリティ対策を中心に述べる。Red Hat Linux は米 Red Hat 社で開発された Linux であり、多数の Linux ディストリビューションの中でも最大のシェアを持つ。豊富なプログラムが RPM (Red hat Package Manager) として利用しやすい形式で提供されている等、使い易さが考慮されている。

しかしながら、経験の浅い管理者でもシステムが容易に構築できるため、ほぼインストール時のデフォルト状態のままインターネットに接続されている例も少なくない。

2.1. 対策の概要

2.1.1. Linux 環境における不正アクセス対策の概要

Linux 環境における基本的なセキュリティは、他の環境と同様に、導入時対策と日常的な管理対策によって実現される。ここでは詳述はしないが、サイトのセキュリティポリシーとシステムの利用計画に添う形で、不要なサービスの削除あるいは停止、初期設定の適正化、アクセス権設定、既知の脆弱性に対する修正プログラムの適用等を行う必要がある。

脆弱性の発見から対策手段の提供までの期間はベンダによってまちまちである。代表的なディストリビューションである RedHat Linux に関しては、SecurityFocus (Bugtraq) 等での脆弱性の公開から、応急的な対策手法の提供あるいは修正プログラムの提供までの期間は比較的短い。この期間は今後更に短縮されるものと思われる。

2.1.2. 対策情報の入手

これまでに良く知られた脆弱性への対策や、サーバ導入時に必要な対策に関する情報源としては以下のサイトが利用できる。各サーバ製品は導入時に製品ベンダのサイトを参照し、脆弱性に関する情報の場所と更新頻度を確認しておくべきである。管理者はユーザ登録により連絡を受けられるように取り計らうことや、サポート情報のチェックを習慣的に行う必要がある。

(1) 日本の Linux 情報

URL : <http://www.linux.or.jp/security/>

深刻なバグやセキュリティに関するニュース (情報源へのリンク)、各ディストリビューションのパッケージ更新に関する情報、インストール直後に取るセキュリティ対策、セキュリティ関連サイトへのリンク集からなる。

(2) Linux Security Knowledge Base

URL : <http://www.securityportal.com/lskb/>

Linux セキュリティに関する総合サイト。膨大な情報が管理者視点のキーワードごとに項目建てられデータベース化されている。

(3) Linux Help Online Security Resources

URL : <http://www.linuxhelp.org/security.shtml>

Redhat、SuSE、Debian 等の Linux ディストリビューションに関するセキュリティ勧告の重要度とリンクを示したリスト、Linux で利用可能なプログラムの脆弱性に関して討議を行う ML、リンク集などからなる。

(4) Debian GNU/Linux セキュリティ情報

URL : <http://www.debian.org/security/>

詳細な警告へのリンクが張られている。警告からは各バージョンの Debian に対応する差分ソースコードや修正パッチへのリンクを辿ることが出来る。

(5) redhat.com Red Hat Linux Errata (英語)

URL : <http://www.redhat.com/support/errata/index.html>

バージョンごとに以下のサイト内の情報へのリンクが示されている。

- ・ セキュリティ勧告 (Security Advisery)
- ・ バグ修正 (Bug Fixes)
- ・ セキュリティ機能を強化するパッケージ (Package Enhancement)

Security Advisery はシステムセキュリティ上修正が不可欠な脆弱性への対策方法を解説し、修正プログラムを取得できる。Bug Fixes はシステムパフォーマンスを向上させるための修正策を示している。PackageEnhancement としては Kerberos パッケージや暗号機能パッケージが挙げられている。

(6) Updates for Vine Linux

URL : <http://vinelinux.org/errata.html>

Vine Linux に関する更新、障害、セキュリティに関する情報がまとめられている。各プラットフォームについてこれまで出された修正済パッケージ / ファイル名、取得可能なミラー、関連する URL (Redhat サイトへのリンク) が示されている。

2.1.3. その他のベンダが提供する UNIX のセキュリティに関する情報

(1) FreeBSD Security Information

URL : <http://www.freebsd.org/security/security.html>

FreeBSD に関するセキュリティ勧告と管理上の Tips 集、セキュアなプログラミングを行うためのガイドが示されている。

(2) Sun Security Information

URL : <http://sunsolve.sun.com/pub-cgi/show.pl?target=security/sec>

Sun 製品のセキュリティに関する公表情報のアーカイブを利用できる。

(3) hp IT resource center hp-ux forums – security

URL : <http://forums.itrc.hp.com/cm/CategoryHome/1,1147,155,00.html>

hp のセキュリティに関する議論のための掲示板である。

2.2. Red Hat Linux オペレーティングシステムの脆弱性とその対策

2.2.1. 管理者権限の不正取得への対策

以下に、Red Hat Linux オペレーティングシステムに存在する脆弱性に基づいた、管理者権限を不正取得するための攻撃手法と、その対策を示す。

(ア) dump におけるバッファオーバーフローに関する脆弱性 (CVE-2000-0186)

手法：ファイルバックアップユーティリティ dump の脆弱性。dump は Redhat では root に setgid されている。「-f a」引数にサイズを超えたパラメータを与えるとスタックオーバーフローを起こしクラッシュする。この際に引数を仕組んでおくと、スタック中の EIP(インストラクションポインタと戻りアドレス)を意図的な実行コードに置き換えることが可能である。ローカルな攻撃者は実行グループ ID の権限を取得できる。

対策：アクセス権の変更。またはパッチの適用。

(イ) makewhatis のシンボリックリンク攻撃 (CVE-2000-0566)

手法：UNIX man ユーティリティに含まれる makewhatis は、/tmp ディレクトリに規則的なファイル名を用いてファイルを作成する。/tmp に作成されるファイルにシンボリックリンクを作成しておくことで、権限の無いファイルにアクセスしたり、アクセス権限を高めたりするなどの symlink 攻撃が行える。ローカルユーザは権限の無いファイルへのアクセスや、ユーザ自身のアクセス権限の向上が可能である。

対策：Linux ディストリビュータが提供する man ユーティリティのアップグレード版をインストールする。

(ウ) rpcd.stated におけるバッファオーバーフローに関する脆弱性 (CVE-2000-0666)

手法：rpc.statd デーモンのログ生成コードはユーザが指定するフォーマット・ストリングを syslog()関数に渡す。攻撃者はプロセスのアドレス空間内に実行コードを送り、バッファオーバーフローによって関数のリターンアドレスを上書きすることで、そのコードを実行させることができる。リモートの攻撃者は任意のプログラムをルート権限で実行可能である。

対策：バージョン 0.1.9.1 以降の nfs-utils をインストールする。

(エ) suidperl におけるエスケープシーケンス攻撃に対する脆弱性 (CVE-2000-0703)

手法：suidperl (spearl) は、エラーレポート送信時に/bin/mail を起動する際に、エスケープシーケンス「~!」を正しく取り除かない。特定の環境変数を設定し、エス

ケーブシーケンスを含むファイル名を引数として `suidperl` を起動することで、ローカルユーザはホストに対してプロセス権限を取得可能である。

対策： `suidperl` が必要なければ、その `setuid` ビットをオフにしておく。RedHat のパッチバージョンでは `/bin/mail` が環境変数を継承する設定を外しているが、 `~/.mailrc` の `set interactive` 行の変更により環境変数の設定をオンにすることができる。

(オ) 複数のシェルのリダイレクトによるシンボリックリンク攻撃に関する脆弱性 (CAN-2000-1134)

手法： `tcsh`、`csh`、`sh`、`bash` において<<リダイレクト (ヒアドキュメント) により一時ファイルを作成する際に、上書きの危険性を考慮せずに予測可能な命名規則に基づいてファイルを作成してしまう。ローカルな攻撃者は事前にシンボリックリンクを張っておくことで他のファイルを上書き、その権限を変更することが可能となる。

対策：ベンダの提供する修正プログラムの適用 (RHSA-2000-117、RHSA-2000-121)

2.2.2. サービス妨害攻撃への対策

以下に、Red Hat Linux オペレーティングシステムに存在する脆弱性に由来するサービス妨害攻撃の手法とその対策を示す。

(ア) `pam_console` モジュールにおけるコンソールユーザ権限奪取に関する脆弱性 (CVE-2000-0668)

手法： `Xdm`、`gdm`、`kdm` 等のディスプレイ・マネージャにおいて XDMCP が有効な場合にリモートからシステムコンソールへのアクセスが可能になり、リブートコマンドが実行可能である。

対策：PAM パッケージをバージョン 0.72 以降にアップグレードする。

2.3. Red Hat Linux のセキュリティ管理

Red Hat Linux を用いてインターネットに接続されたサーバを構築する上での注意点を以下に示す。

2.3.1. デフォルトのアカウントに関する修正

デフォルトで存在するユーザアカウントに対して適切なパスワードを設定し、不要なアカウントは削除あるいはロックする。利用するユーザアカウントには予測困難なパスワードを設定する。単語、単語の逆さ読み、誕生日等の数字、業界用語や外国語などは推測が容易なので避ける。パスワードを人に教えたり、容易に目にすることができる場所に書きつけたりしてはいけない。また、パスワードは頻繁に更新することが望ましい。

2.3.2. 既知のセキュリティホールへの修正

欠陥の修正された最新のプログラムを使用する。kernel、sendmail、apache、ftp、bind 等は頻繁に更新される重要なプログラムであるため、特に注意を要する。Web サーバとしての視点から特に重点的な対処が必要な箇所としては syslogd、glibc、mailx、perl、RPM、PAM packages、man、wu-ftpd、kernel などが挙げられる。

2.3.3. 不要なサービスの停止と削除

不要なサーバプロセスは起動するべきではない。導入時に必要なサービスを十分に検討し、不要なサービスはインストールの対象から外す。サービス数が増えるほどセキュリティ対策に多くの労力が必要になり、運用するサービスの見落としにも繋がる。脆弱性対策を施さずに放置されたサービスは攻撃者の侵入路になりやすい。

各種のインターネットサービスに対して外部からポートに送られてくる要求はインターネットスーパーサーバ (inetd) が見張っている。inetd から起動されるデーモンは/etc/inetd.conf に記されている。この/etc/inetd.conf を参照し、不要なサービスは#でコメントアウトし停止する。コメントアウトが必要な行の例としては systat、netstat、chargen、finger、discard を起動する行が挙げられる。

現在実行されているサーバプロセスの把握には ps auxw、netstat -a コマンドを用いる。不要なサーバプロセスは、/etc/rc.*ファイルを編集し OS 起動時に起ち上がらないようにする。メールサーバとして運用しない場合は sendmail を、ファイルサーバではない場合は nfs を停止することが望ましい。不要なサービスの停止には ntsysv、chkconfig コマンドを用いる。

Web サーバとして稼働させておくべき最低限のサービスとしては crond、httpd、inet、keytable、network、random、syslog が挙げられる。

2.3.4. root のセキュリティ

root (スーパーユーザ、管理者) アカウントは、そのマシン全体に対する権限を持ち、ネットワーク上の他のマシンに対する権限を持つこともある。このため、root アカウントの取得は攻撃者の最大の目標とされる。

root アカウントは可能な限り短時間の特定の作業のみに用い、他の作業は一般ユーザとしてマシンを使用すべきである。root でログイン中に起こしたちょっとしたミスがシステムの全体に及ぶ大きな問題となり得る。root としての作業が必要な場合は、root になる前に作業内容を明確にし、計画的な作業を行うことが望ましい。

(1) root になれるユーザの制限

インストール直後の状態では、誰でも su コマンドで root になることを試行可能である。これをグループ root に所属するユーザのみが root になる権限を持つように変更する。/etc/group を編集して root 権限を与えたいユーザをグループ root に加え、/etc/login.defs の SU_WHEEL_ONLY の部分を yes にする。(この対策が施せない login パッケージも存在する)

(2) リモートホストからの root ログインの無効化

/etc/securetty には root がログインできる端末のリストが書かれている。Red Hat Linux のデフォルトでは、ローカルの仮想端末 (vty) だけが設定されている。このファイルに他の端末を追加するときには細心の注意が必要となる。

リモートから root として作業する必要があるときは、ssh 等の暗号化チャネルを利用して一般ユーザとしてリモートログインし、その後に su コマンドを用いて root 権限を得ることが望ましい。

(3) root による rlogin、rsh、rexec 等の r-コマンド群の禁止

これらは信頼関係のあるリモートホスト間で安全な通信路が確保されている場合の利用が前提になっているため、致命的な攻撃の対象となる。これらのコマンドを root で実行すると非常に危険である。r-コマンドで信頼されるホストは.rhosts ファイルには記載されるが、root ユーザ用の.rhosts ファイルは決して作ってはいけない。

(4) ワイルドカード (*や?など) の使用に関する注意

ワイルドカードでの指定には想定外のファイルの削除が起きる可能性や、対象に攻撃者によって置かれたプログラムやデータが含まれる可能性がある。root 権限を持つときには指定はできるだけ厳密に行い、対象範囲を明確にするためには ls コマンド等で確認を取る。

(5) root ユーザ用のコマンドパスの制限

「.」(カレントディレクトリ) を PATH の指定に絶対に含めてはいけない。また、書き込み

可能なディレクトリを検索パスに加えると、root 権限でトロイの木馬プログラムを起動する可能性がある点には注意が必要である（検索パス上の検索の優先順位がより高い同名ファイルが存在するかもしれない）。

2.3.5. TCP_wrapper によるサービスへのアクセス制限

インターネットスーパーサーバ (inetd) から起動するサービスへのアクセスを制限するためには TCP_wrapper (tcpd) が用いられる。TCP_wrapper は inetd が接続要求を監視しているさまざまなサービスに対して覆い被さるようにして動作する。通常、インターネットサービスへの接続要求は inetd からサービスのデーモンに直接渡されるが、TCP_wrapper は inetd から要求をいったん受け取り、接続要求の許可/不許可を定義に基づいて判定し、許可する場合のみインターネットサービスに接続を渡す。TCP_wrapper の適用が望ましいサービスとしては、telnet、ftp などがあげられる。

TCP_wrapper によるアクセス制御のルールは、アクセス許可ファイル/etc/hosts.allow とアクセス拒否ファイル/etc/hosts.deny で定義される。各ファイルにはアクセス制御対象となるサービス名とホスト（ホスト名あるいは IP アドレス）が記述される。どちらのファイルにも記述されていないアクセスは許可されてしまう。両方に含まれているアクセスは許可される。そこで、抜けや落ちのない制御を行うためには以下のように記述する。

- ・ /etc/hosts.deny ファイルには全てのアクセスを拒否
- ・ /etc/hosts.allow ファイルには内部ネットワークと特定のホスト/ドメインからのアクセスのみを許可

2.3.6. ssh の利用

ssh は、telnet や r-コマンド (rsh、rcp など) のより安全な代用品として、セキュアな認証や TCP コネクションを単位とした通信の暗号化を行うものである。

telnet や r-コマンドでは認証時のパスワードや、その後続くデータが平文で送られている。このためパスワードの漏洩や、セッションハイジャックの危険がある。

ssh でリモートシステムに接続する際には、まずホスト間に暗号化された通信路が確立され、次にセキュアなプロトコルに基づいたユーザ認証が行われ、パスした場合に暗号化された接続が続けられる。

また、ssh は X プロトコル (X-Window で使われる IP パケット) を暗号化する機能や、ポートフォワーディングにより POP3 等の他のポートを利用した通信を暗号化する機能を持つ。

2.3.7. メール関連設定

sendmail およびその他のメール転送エージェント (MTA) に関する不正アクセス手法と対策について述べる。

sendmail は広く使われているメール転送エージェントプログラムである。高い拡張性を持ち高度な構成が可能である。sendmail はコードが 8 万行におよぶ巨大で複雑なプログラムであり、これまでに数多くのセキュリティ上の弱点が報告されている。sendmail は設定が困難なことで知られている。

(1) 旧バージョンの sendmail

管理者は sendmail については、セキュリティ情報を常に収集し、必要であるなら設定の変更や最新バージョンのプログラムへの更新が求められる。

旧バージョンの sendmail は、メールの中継を認めるデフォルト設定が施されている点、プログラムにバッファオーバーフローに関する脆弱性が存在する点など、多くの問題を抱えている。これらの弱点は非常に良く知られた致命的なものであり、放置すればメールサーバへの侵入や不正な中継利用を受ける原因となる。

以下に各バージョンの sendmail の持つ問題とその対策をまとめる。

- ・ 5.x で表されるバージョンの sendmail (R5 sendmail) には多くの致命的なセキュリティホールが存在することが知られている。旧バージョンであれば攻撃者にサーバ情報を収集された場合に、極めて魅力的な攻撃対象と見なされ得る。また、旧バージョンのプログラムは適切なサポートを受けらず、脆弱性を修正することが全くできない場合もある。このような理由から、8.x.x で表されるバージョンの sendmail (R8 sendmail) の中で入手可能な最新のバージョンへ可能な限り早く変更する必要がある。
- ・ sendmail-8.8.x 以降にはスパム対策および踏み台対策のための設定内容をチェックするツール check_relay が付属する。
- ・ 8.8.8 以前の sendmail は第三者によるメールの中継を許可する設定がデフォルトで取られているため、それらのバージョンの sendmail が導入されている場合はスパム対策のための設定と動作確認が必須である。
- ・ sendmail-8.9.0 以降ではデフォルト時の sendmail.cf ファイルに第三者からのメールの中継を行わないよう設定されている。
- ・ 8.9.0 以降のバージョンの sendmail についてもいくつかの脆弱性が指摘されている。Bugtraq (<http://www.securityfocus.com>) 等で脆弱性に関する最新情報を集める必要がある。

(2) 不正アクセス対策

sendmail の利用に際しては、入手可能な最新バージョンのプログラムを導入して適切な設定を慎重に施す必要がある。sendmail は歴史のある有名なプログラムであるが、導入後に脆弱性が報告される可能性は未だにある。脆弱性情報に注意を払う必要が特にあるプログラムの 1 つである。可能ならば最新のプログラムを導入すべきである。

sendmail に関する不正アクセス対策項目を以下に示す。

- ・ メール受信に利用していない不要な sendmail サービスの停止、プログラムの削除
- ・ 最新バージョンの sendmail の導入
- ・ スпамメールの不正中継配信への対策
- ・ サービス妨害攻撃への対策
- ・ サーバのアカウントに関する情報列挙への対策

sendmail の設定に関しては、定義ファイル sendmail.cf は難解な記述方法で書かれている。設定変更時にこのファイルを直接編集することは極めて困難なので、条件を判りやすく記述したファイルから sendmail.cf を自動的に作成するツール CF を用いる。

2.3.8. Web 関連設定

Web 関連の設定としては Apache の設定があげられる。Apache は UNIX 環境でフリー / 商用を問わず広く使われている Web サーバソフトウェアである。Linux には標準の Web サーバとしてパッケージに含まれている。以下に Apache に関するセキュリティ上の対策について述べる。

(1) Apache の設定

Apache の設定について重要な項目を以下に挙げる。

(ア) インストール時

- ・ 最新のバージョンの Apache を入手して用いる。
- ・ Web 管理用のユーザアカウントを作成する：
Web サービスに無関係なシステムに対して管理作業時に誤った操作を施す危険を避けられる。
- ・ インデックス表示の禁止：
アクセス制御ディレクティブの<option>から "Indexes" を削除する

(イ) CGI

- ・ httpd.conf で CGI を実行するディレクトリを指定することができる。このディレクトリのアクセス権限の設定には注意すること。制限が適切でなければ意図しないプログラムのインストール、ソースコードやデータファイルの露呈といった危険が予想される。
- ・ ユーザディレクトリでの CGI の実行を許可すると、管理者が把握できない危険性がサーバ上に存在することになる。サーバ全体のセキュリティ上の弱点となる点には注意が必要である。
- ・ 外部から入手した CGI プログラムには、悪意あるコードが含まれている危険性や、脆弱性が存在する危険性がある。十分なコードのチェックを行うか、信頼のおける配布元からの供給を受けたコードを用いる必要がある。

(ウ) SSI

- ・ CGI に比べより大きな危険となる可能性がある。
- ・ SSI を利用しない場合は利用できないような設定を必ず行う。
- ・ SSI を実行するディレクトリは完全に把握する必要がある。
- ・ SSI を実行するファイルの拡張子は shtml に限定する。意図しない SSI の使用を防ぐ効果がある。
- ・ SSI を使う場合でも exec 関連の include は禁止する。これを許すと攻撃者がフォー

ムに書き込んだ SSI 行が SSI 解析前に適切に削除されなければ任意のコマンドを実行される危険がある。

(2) Apache に関する脆弱性と影響を受けるバージョン

以下に Apache に関する脆弱性と、その脆弱性の影響を受けるバージョンを示す。

脆弱性の影響を受けない新しいバージョンの Apache プログラムを用いることが、これらの脆弱性に基づく攻撃への予防対策となる。

ディレクトリ内要一覧表示に関する脆弱性

- ・ 膨大な数のスラッシュを使った長いパス名のリクエストを送ることでディレクトリの内容一覧を取得可能。リモートからの攻撃者は情報収集が可能。
- ・ 対象バージョン：Apache 1.3.19 以前
- ・ 参考：BID:2503

PHP3 のファイル露呈に関する脆弱性

- ・ PHP が動作する Apache1.3 において、ディレクトリ横断の手法を用いたリクエストにより Web サーバのルート配下に置かれたファイルを取得できる。リモートからの攻撃者は既知のファイル名を持つファイルを取得可能。
- ・ 対象バージョン：Apache 1.3.6
- ・ 参考：CAN-2001-0042、BID:2060、XF:apache-php-disclose-files(5659)

Rewrite モジュールのファイル露呈に関する脆弱性

- ・ Apache 1.2 以降に含まれる mod_rewrite モジュールの脆弱性。正規表現のファイルネームを含むように RewriteRule ディレクティブが拡張されている場合に、リモートからの攻撃者はホスト上の任意のファイルを取得することが可能。
- ・ 対象バージョン：Apache 0.8.11、Apache 0.8.14、Apache 1.0、Apache 1.0.2、Apache 1.0.3、Apache 1.0.5、Apache 1.1、Apache 1.1.1、Apache 1.3.11win32、Apache 1.3.12
- ・ 参考：BID:1728、CVE-2000-0913、XF:apache-rewrite-view-files(5310)

SuSE Apache WebDAV のディレクトリ一覧表示に関する脆弱性

- ・ デフォルトの設定では WebDAV が有効になっている。PROPFIND HTTP リクエストを送ることで、リモートからの攻撃者は任意のディレクトリの一覧を取得可能。
- ・ 対象バージョン：Apache 1.3.12
- ・ 参考：BID:1656、CVE-2000-0869

Windows 版 Apache におけるルートディレクトリアクセスに関する脆弱性

- ・ リモートからの攻撃者はディレクトリの一覧を取得可能。ディレクトリの一覧表示が config で許可されていて、index ファイルが存在するときでも一覧が表示される。
- ・ 対象バージョン : IBM HTTP Server 1.3.3 win32、IBM HTTP Server 1.3.6.2 win32、Apache 1.3.12 win32 以前
- ・ 参考 : BID:1284、CVE:CVE-2000-0505

ScriptAlias ソース露呈に関する脆弱性

- ・ ScriptAlias ディレクトリが DocumentRoot 以下に置かれていた場合に、リモートからの攻撃者は cgi-bin ディレクトリの下プログラムソースコードや機密情報を取得可能。
- ・ 対象バージョン : Apache 0.8.14 以前、NSCA httpd 1.5a-export 以前
- ・ 参考 : BID:2300、CVE:CVE-1999-0236

MIME ヘッダによるサービス妨害攻撃に対する脆弱性

- ・ リモートからの攻撃者は 8000 バイトにおよぶ長い MIME ヘッダを大量に送信することで Web サービスをクラッシュさせることができる。通常の機能の回復にはサービスの再起動が必要。
- ・ 対象バージョン : Apache 1.2.5、Apache 1.3.1、MessageMedia UnityMail 2.0
- ・ 参考 : BID:1760

GET リクエストを用いたサービス妨害攻撃に対する脆弱性

- ・ リモートからの攻撃者は大量の「/」文字を含めた大量の GET リクエストを送信することでバッファオーバーフローを起こすことができる。サーバをフリーズさせてサービスの妨害を試みる事が可能。通常の機能の回復にはサービスの再起動が必要。
- ・ 対象バージョン : Apache 1.2.5 以前
- ・ 参考 : BID:2216、CVE:CAN-1999-0107

mod_cookies のバッファオーバーフロー - に関する脆弱性

- ・ Apache httpd におけるクッキー処理関連プログラムの脆弱性。mod_cookies.c 中の make_cookie 関数に適切なチェックを行っていないバッファが存在する。リモートからの攻撃者はバッファオーバーフローを起こすことで、サーバへのアクセス権を取得可能。
- ・ 対象バージョン : Apache 1.1.1 以前
- ・ 参考 : NAI:NAI-2、XF:http-apache-cookie、BID:1821、CVE-1999-0071

nph-test-cgi スクリプトに関する脆弱性

- ・ デフォルトでインストールされる nph-test-cgi プログラムに脆弱性が存在する。リモートからの攻撃者はサーバ上のファイルの一覧を取得可能。
- ・ 対象バージョン：NCSA NSCA httpd 1.5.2a 以前、Apache 1.1 以前、Netscape Commerce Server 1.12、Netscape Communications Server 1.1/1.12、Netscape Enterprise Server 2.0a
- ・ 参考：CERT:CA-97.07.nph-test-cgi_script、CVE:CVE-1999-0045、XF:http-cgi-nph、
BID:686、

test-cgi スクリプトに関する脆弱性

- ・ デフォルトでインストールされる test-cgi プログラムに脆弱性が存在する。リモートからの攻撃者はサーバ上のファイルの一覧を取得可能。
- ・ 対象バージョン：NCSA NSCA httpd 1.5.2a 以前、Apache 1.0.5 以前
- ・ 参考：XF:http-cgi-test、BID:2003、CVE:CVE-1999-0070

phf スクリプトに関する脆弱性

- ・ CGI phf プログラムに致命的な脆弱性が存在する。リモートからの攻撃者はシェルメタキャラクタを利用して任意のコマンドの実行が可能。
- ・ 対象バージョン：Apache 1.0.3、NSCA httpd 1.5a-export
- ・ 参考：CERT:CA-96.06.cgi_example_code、XF:http-cgi-phf、CVE:CVE-1999-0067、
BID:629